REMARKS

In response to the Office Action mailed July 17, 2006, Applicant respectfully request reconsideration. Claims 1-9 were previously pending in this application. Claims 1 and 8 have been amended. New claims 10-14 have been added. As a result, claims 1-14 are pending for examination with claims 1, 8, and 10 being independent. No new matter has been added.

I. Overview of Embodiments of the Invention

One embodiment described in the application is directed to a method for protecting the operations of a ciphering/deciphering circuit from attacks by external power analysis by inserting random numbers into various points in an encryption/decryption process performed by the ciphering/deciphering circuit. In one exemplary implementation, two randomly-generated numbers are used, and are inserted into calculations related to the encryption/decryption process such that a result is achieved that would be identical to a result of the process if the random numbers were not inserted at all. While other prior art systems use one number or multiplication to achieve this end, this embodiment of the present application lowers execution time and memory constraints by using two random numbers, applied using XOR-type gates, each being comprised of repeated sequences of a single byte.

The foregoing summary is provided solely for the convenience of the Examiner. It should be appreciated that each of the independent claims may not be limited in the manner described in the summary above. Therefore, the Examiner is requested not to rely upon the summary for determining whether each of the claims distinguishes over the prior art of record, but to do so based solely on the language of the claims themselves and the arguments presented below.

II. Objections to the Specification

The Office Action objected to the disclosure because of the following informalities: *On page 10, line 10, the following has been recited. "SR(S_i) + SR." It should be corrected as "SR(S_i) + SR (R)".*

Applicants have herein amended the specification as requested, and thank the Examiner for identifying the error. Amendments can be found on page 2 of this paper.

Accordingly, withdrawal of this objection is respectfully requested.

III. Claim Rejections under 35 U.S.C. §112

The Office Action rejects independent claim 1 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular, the Office Action states that "*Independent claim 1, recites the limitation '...the operands.' There is insufficient antecedent basis for this limitation in the claim. The term 'operands' has to somehow be defined in the claim.*"

Applicants have amended claim 1 to recite "masking input and output blocks of the non-linear transformation" rather than "masking the operands." Accordingly, withdrawal of this rejection is respectfully requested.

Independent claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular, the Office Action states that "*Independent claim 8 recites the limitation 'non-linear transformation (34, 54).' This limitation raises a question whether or not it actually refers to the disclosure/diagram.*"

Applicants respectfully draw the Examiner's attention to the preliminary amendment filed by Applicants on July 1, 2003, in which the noted recitation in claim 8 was cancelled. Accordingly, withdrawal of this rejection is respectfully requested.

IV. Claim Rejections - 35 USC § 103

Claims 1-9 are rejected under 35 U.S.C. 103(a) as being allegedly obvious over admitted prior art, in view Snell, US Publication No. 2003/0223580 Al. Applicants traverse these rejections, and have amended independent claims 1 and 8 not to overcome these rejections, but solely to address informal issues noted elsewhere herein, and to improve readability of the claims.

A. Overview of Admitted Prior Art

Admitted prior art discloses methods for protecting a circuit employing an Advanced Encryption Standard algorithm to cipher and decipher data by using random variables to mask the data (Applicants' specification, Page 4, lines 3-7).

In one method, illustrated in FIG. 3 of the disclosure, a masking operation is implemented wherein a random number is combined bit by bit using an XOR gate with the data

to be encrypted at several points in the encryption process (Page 4, lines 10-13). There are no requirements imposed on this random number. By combining the data and the random number at several points, the masking operation can be done and undone in such a way that the encryption process yields the same encrypted result as it would without the random number, while protecting against an attack by external power analysis (Page 4, lines 21-23). Combination with the random number in this way, however, necessitates use of a substitution box calculated based on the random number, which lengthens the execution time of the encryption and noticeably increases the memory requirements (Page 4, lines 24-31).

In a second method according to the admitted prior art, illustrated in FIG. 4 of the disclosure, two random number are used, again combined with the data at various points in the encryption algorithm. Again, there are no requirements imposed on these random numbers. The first random number is combined with the unencrypted data at the beginning of the process using an XOR-gate (Page 5, lines 9-11), and only applied again at the end of the process (Page 5, lines 28-29). It is never used in the intermediary steps or combined with the intermediary encrypted data. The second random number is multiplied with the intermediary encrypted data at several points in the encryption process (Page 5, lines 13-15 and lines 22-24). Such multiplication becomes complex and requires many operations, significantly lengthening the execution time of the algorithm (Page 6, lines 4-7).

B. Overview of Snell

Snell discloses a method and circuit for combating attacks on an encryption system by external power analysis through a masking operation using a random number (Snell, paragraph 18). To do so, Snell uses a dummy circuit separate from the encryption circuit that performs calculations on a randomly-generated number of the same width as the data to the ciphered (Paragraph 18). In Snell the only requirement on the randomly-generated number is this matching size, such that it is difficult for an attacker to separate the power signature of the dummy circuit from that of the legitimate calculations (Paragraph 85). This randomly-generated number is not mixed with the legitimate data for encryption, but is only used in Snell's separate dummy circuit for obfuscation of the overall circuit's power signature (Paragraph 85).

C. Claims 1-7 and 9

Applicants' independent claim 1, as amended, recites a cyphering/decyphering method, by an integrated circuit, of a digital input code by means of several keys. The method comprises: dividing said code into several data blocks of same dimensions; applying to said blocks multiple turns of a cyphering or decyphering comprising submitting each block to at least one same non-linear transformation and of subsequently combining each block with a different key at each turn, and masking inputs and outputs of the non-linear transformation, upon execution of the method, by means of at least one first random number having the size of said code and all the blocks of which have the same value by combining, by an XOR-type function, the input and output blocks of the non-linear transformation with said random number.

As set forth in MPEP §2143, three criteria must be met in order to establish a *prima facie* case of obviousness. First, there must be some suggestion or motivation, either in the cited reference(s) or in the knowledge generally available to one of ordinary skill in the art, to modify the cited reference(s) or to combine reference teachings (if multiple references are cited). Second, there must be a reasonable expectation of success. The teaching or suggestion to modify the reference(s) or to combine reference teachings as well as the reasonable expectation of success must both be found in the prior art and not based on Applicants' disclosure. Third, the prior art reference(s), when viewed as a whole, must teach or suggest all of the claimed features. Failure to meet any one of these criteria – a teaching or suggestion of all claim elements, a specific suggestion or motivation to modify or combine the prior art, and a reasonable expectation of success – is sufficient to render an obviousness rejection improper.

As discussed below, *none* of these three criteria is met in the rejection of claim 1 over the combination of the admitted prior art and Snell.

1. The suggested combination does not teach all elements of the claimed invention.

The admission of prior art in view of Snell does not teach or suggest all the limitations of claim 1. Specifically, there is no disclosure in either the admitted prior art or in Snell regarding the specific contents of the random numbers. Claim 1 is limited to a random number in which all the blocks have the same value. The random numbers of Snell and the admitted prior art are not limited in this way. The Office Action asserts on page 4 that this limitation is taught in

Applicants' admission of prior art, but the methods describe in the background of the instant application do not disclose any such requirement. Both the admitted prior art and Snell simply disclose generating random numbers of a necessary length—Snell going one step further, requiring that the length of the random number equal that of the data to be ciphered—but neither reference discloses that the contents of the random number be limited to one in which all the blocks have the same value. Since claim 1 does recite a limitation on the contents of the random number, neither the admitted prior art nor Snell, alone or in combination, teaches all elements of claim 1, as required by MPEP §2143.

For at least the foregoing reasons, the admitted prior art and Snell, alone or in combination, fail to teach or suggest all claim limitations. Accordingly, the Office Action has failed to establish at least this criterion of a *prima facie* case of obviousness as set forth in MPEP §2143.

2. There is no suggestion or motivation to combine the references.

The Office Action alleges that a person of ordinary skill in the art would have been motivated to "add the features of the circuit wherein the pseudo-random generator and XOR array of the dummy circuit having a word width in bits identical to that of pre-mix subcircuit in the which [sic], it is configured to perform AES ... as per teachings of Snell to the method as taught by Admission, in order to counteract differential power analysis attacks in symmetric key block cipher algorithms such as AES/Rijndael." Applicants respectfully disagree that a person of ordinary skill in the art would have been so motivated.

The admitted prior art specifically discloses "known solution[s] to make the algorithms more resistant against differential power analysis attacks of the integrated circuit" (Applicant's specification, page 4, lines 3-4). Additionally, The algorithms disclosed are AES/Rijndael. Therefore, there is no explicit or implicit need for modifying the admitted prior art as the Office Action suggests. Further, the prior art of record does not disclose or suggest any desirability for modifying the random numbers to be mixed with the encrypted data in the admitted prior art, so as to make use of Snell's matched word width. As stipulated in MPEP §2143.01, "The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination." The admitted prior art does

not disclose any motivation for restricting or setting the size of the random numbers to be mixed into the disclosed encryption processes, a point the Office Action concedes on page 5.

Thus, one of ordinary skill in the art, upon examining the admitted prior art of Applicants' disclosure, would *not* be motivated to make the modification suggested by the Office Action, since there does not exist a need for the modification nor any reasonable suggestion in the prior art to do so. For at least the foregoing reasons, there is no suggestion or motivation to combine the admitted prior art and Snell, and again a *prima facie* case of obviousness has therefore not been established pursuant to MPEP § 2143.

3. There is no reasonable expectation of success.

The Office Action fails to specify any indication, either in the references themselves or in the knowledge generally available in the art, of a reasonable expectation of success in combining the admitted prior art and Snell. Most notably, the Office Action completely fails to specify or suggest in any manner *how* one of ordinary skill in the art would practically and realistically combine various elements of the admitted prior art and Snell to successfully arrive at an apparatus or method that would resemble the subject matter of Applicants' claims. Instead, the Office Action merely provides a general assertion of an alleged motivation to combine the references, without any specific support or discussion of a reasonable expectation of success in combining the references.

In view of the foregoing, it is entirely unclear from the admitted prior art and the Snell reference how the different elements of these references would realistically be combined to provide a viable functioning device. Not only do the references, when viewed as a whole, fail to provide any such teaching, suggestion or motivation, but furthermore the Office Action provides no insight as to how to practically and successfully implement such a combination.

4. For each of the three reasons set forth above, no *prima facie* case of obvious has been established.

In view of the foregoing, the admitted prior art and Snell, either alone or in combination, fail to disclose or suggest all of the features of claim 1. In addition, there is no suggestion or motivation to combine the admitted prior art and Snell, and no reasonable expectation of success. Accordingly, claim 1 patentably distinguishes over the combination of the admitted prior art and

Snell and is in condition for allowance. Claims 2-7 depend from claim 1 and are allowable for at least the same reasons. Therefore, it is respectfully asserted that the rejection of claims 1-7 under §103 as allegedly being obvious over admitted prior art in view of Snell is improper and should be withdrawn.

D. Claims 8-9

Applicants' independent claim 8, as amended, recites an integrated circuit for cyphering/decyphering by turn input data divided into blocks of same dimensions. The circuit comprises: means for generating at least one first random number, comprised of a repeated sequence of a value, of same size as the size of the blocks of the input data; and means for combining said random number with each block, at an input and at an output of a non-linear transformation implemented by the cyphering/decyphering.

For reasons that should be clear from the above discussion in conjunction with claim 1, the admitted prior art in view of Snell does not teach or suggest all the limitations of claim 8. Specifically, the admitted prior art in view of Snell does not disclose a random number *comprised of a repeated sequence of a value*. There is no teaching or disclosure in either the admitted prior art or in Snell regarding the specific content of the random number.

Further, for reasons that should again be clear from the above discussion in conjunction with claim 1, one of ordinary skill in the art simply would not have been motivated to combine the admitted prior art and Snell and there would be no reasonable expectation of success in implementing such a combination.

In view of the foregoing, it is clear that no *prima facie* case of obviousness has been established. Accordingly, claim 8 patentably distinguishes over the combination of the admitted prior art and Snell and is in condition for allowance. Claim 9 depends from claim 8 and is allowable for at least the same reasons. Therefore, it is respectfully asserted that the rejection of claims 8 and 9 under §103 as allegedly being obvious over admitted prior art in view of Snell is improper and should be withdrawn.

V. General Comments on Dependent Claims

Since each of the dependent claims depends from a base claim that is believed to be in condition for allowance, Applicants believe that it is unnecessary at this time to argue the

allowability of each of the dependent claims individually. Applicants do not, however, necessarily concur with the interpretation of the dependent claims as set forth in the Office Action, nor do Applicants concur that the basis for the rejection of any of the dependent claims is proper. Therefore, Applicants reserve the right to specifically address the patentability of the dependent claims in the future, if deemed necessary.

VI. New claims

New claims 10-14, including independent claim 10, have been added to further define Applicants' contribution to the art. Independent claim 10 recites, *inter alia*, "a random number having the same size as the output and being comprised of a repeated sequence of a value." Thus, these claims also distinguish over the admitted prior art and Snell for at least the reasons discussed above.

CONCLUSION

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment set forth in the Office Action does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Furthermore, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify any concession of unpatentability of the claim prior to its amendment.

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicants' representative at the telephone number indicated below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,

Dated: November 16, 2006

By: */ Joseph Teja, Jr. /*
Joseph Teja, Jr.
Registration No.: 45,157
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
(617) 646-8000